ISSN No. 0976-5697

Volume 7, No. 3, May-June 2016

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Study of RSA, DES and Cloud Computing

Pooja Bindlish
Research Scholar in CSE Deptt.
H.C.T.M College, Kaithal
Kaithal (Haryana), India
poojabindlish.p@gmail.com

Pawan Kumar
Assistant Professor in CSE Deptt.
H.C.T.M College, Kaithal
Kaithal (Haryana), India
pawanspp@gmail.com

Abstract: Now days, security of data become a large concern to insure various attributes like integrity, confidentiality, authentication etc. Cryptography techniques are used for this purpose. It plays a major role in protecting the data in those applications which are running in a network environment. To increase data security cryptography techniques also used on cloud because cloud computing provides secure transmission of data. On cloud, various computing task or programs can be run at a time. Cloud computing provides an illusion to the customers of using infinite computing resources that are available from anywhere, anytime, on demand.

Keywords: Cryptography, Cloud computing, RSA, DES, Encryption, Decryption

1. INTRODUCTION

Cryptography from Greek , "hidden, secret" respectively is the practice and study of techniques for secure communication in the presence of third parties (called adversaries)[1]. Cryptography is used for constructing and analyzing protocols. Cryptography is mainly used for increasing the data security so that data between two parties can be safely exchanged through network without getting leaked. There are various techniques of cryptography but in this paper only two of them were studies i.e. RSA and DES. Key basics of cryptography are that it requires only two components. They are:

1) Algorithm: Steps for doing encryption and decryption
2) Key: Any value that is used for encryption/decryption. For eg.Like key of every vehicle is different to insure that no other key can be used to run that vehicle.

TYPES OF CRYPTOGRAPHY: There are two types of cryptography.

(1) Symmetric-key cryptography

In a symmetric cryptosystem, the same key is used for encryption and decryption.

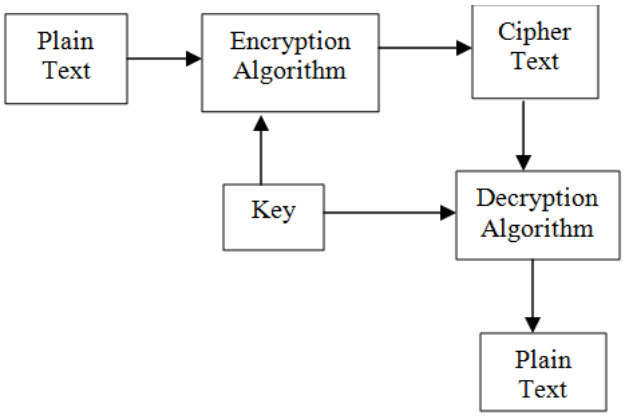


Figure 1: Symmetric key Cryptography

(2) Asymmetric-key cryptography

In an asymmetric, the encryption and decryption keys are different but related. The encryption key is known as the public key and the decryption key is known as the private key. The public and private keys are known as a key pair.

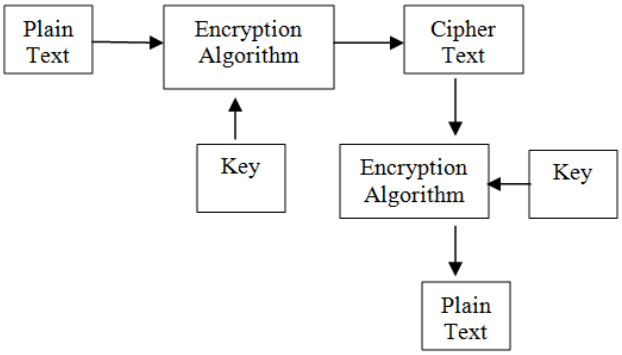


Figure 2: Asymmetric key Cryptography

Cloud computing is a colloquial expression which is used to describe a various types of computing concepts that involve a large number of computers which are connected through a real-time communication network (usually Internet). It is a jargon term with a rejected non-ambiguous scientific or technical definition.As cloud is used to collect the water and rain occur when cloud collide with any solid thing like that cloud computing is used to store and access data over the internet instead of one's computer hard drive.

Cloud Computing Service Delivery Models

Following on the cloud deployment models, the next security consideration relates to the various cloud computing service delivery models[2]. The three main cloud service delivery models are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

2. LITERATURE SURVEY

In this section the work done by the various researchers in the field of cryptographic algorithm and cloud for data security. From this survey various gaps have also been drawn and defined in section 3.

Hung-Min Sun *et al.* [3] proposed dual RSA algorithm and also analyzed the security of the algorithm. The new variants of RSA were presented by them whose key generation algorithms output two distinct RSA key pairs having the same public and private exponents Two applications for Dual RSA were blind signatures and authentication. The security of Dual RSA was raised in comparison to RSA when there were small values of e and d. The main disadvantage of using dual RSA was that the computational complexity of the key generation algorithms was also increased.

P.Saveetha & S.Arumugam[4] worked on the Network Security. According to them the network security as a mean to protect data during their transmission over channel of networks similarly Internet Security also to protect data during their transmission over a collection of interconnected networks in all over the world.Cryptography is the way of hiding information during transmission over a cannel. There are lots of cryptographic algorithms available to protect our data from intruders.RSA also one of effective the public key cryptographic algorithm which needs time and memory.

B.Persis Urbana Ivy et al.[5] worked to secure data or information by a modified RSA cryptosystem based on'n'prime. This is a new technique to provide maximum security for data over the network. It is involved encryption, decryption, and key generation. Prime number used in a modified RSA cryptosystem to provide security over the networks. In this technique we used 'n' prime number which is not easily breakable. 'n' prime numbers are not easily decompose. This technique provides more efficiency and reliability over the networks. In this paper we are used a modified RSA cryptosystem algorithm to handle 'n' prime numbers and provides security.

CRS Bhardwaj[6] discusses the modification of DES algorithm, which is the science of data encryption, a technology that provides for a safe, secure, and private information exchange.PN Generator produce the infinite random numbers which can be used to modify the DES algorithm to make it more critical to decipher. The modified encryption of data cannot be deciphered by DES algorithm. It enables you to send the secure data between two computers on private wireless link.

Shah Kruti R.& Bhavika Gambhava[7] give the principal goal guiding the design of any encryption algorithm must be security against unauthorized attacks. Within the last decade, there has been a vast increase in the accumulation and communication of digital computer data in both the private and public sectors. Much of this information has a significant value, either directly or indirectly, which requires protection. The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. Performance and security level is the main characteristics that differentiate one encryption algorithm from another. Here introduces a new method to enhance the performance of the Data Encryption Standard (DES) algorithm is introduced here. This is done by replacing the predefined XOR operation applied during the 16 round of the standard algorithm by a new operation depends on using two keys, each key consists of a combination of 4 states (0, 1, 2, 3) instead of the ordinary 2 state key (0, 1). This replacement adds a new level of protection strength and more robustness against breaking methods.

Mary Cindy Ah Kioon et al.[8] analyses the security risks of the hashing algorithm MD5 in password storage and discusses different solutions, such as salts and iterative hashing. We propose a new approach to using MD5 in password storage by using external information, a calculated salt and a random key to encrypt the password before the MD5 calculation. We suggest using key stretching to make the hash calculation slower and using XOR cipher to make the final hash value impossible to find in any standard rainbow table.

Priyanka Walia & Vivek Thapar[9] discusses that there have been significant research advances in the analysis of hash functions in past few years and it was shown that none of the hash algorithm is secure enough for critical purposes whether it is MD5 or SHA1.Nowadays scientists have found weaknesses in a number of hash functions, including MD5, SHA and RIPEMD so the purpose of this paper is combination of some function to reinforce these functions and also increasing hash code length up to 512 that makes stronger algorithm against collision attests.

Chong Hee Kim [10] improved differential fault analysis on AES key schedule. Proposed advanced encryption standard for which the main target is known DFA. Implementation of AES is known to be vulnerable to DFA which could be split into two categories depending on the fault location that has the DFA on the state and the DFA on the key schedule. The major limitation is that if the key schedule is not redone for recomputation then it cannot prevent DFA on the AES Key Schedule. The major problem was that if the key schedule was not done again for recomputation then it cannot prevent DFA on the AES Key Schedule.

Abid Shahzad and Mureed Hussain [11] discusses Security Issues and Challenges of Mobile Cloud Computing. Cloud computing is proving itself an emerging technology in IT world which provides a novel business model for organizations to utilize softwares, applications and hardware resources without any upfront investment. Few years later with the broad development in mobile applications and advancements in cloud computing, a new expansion is being expected in the form of mobile cloud computing (MCC). MCC provides a platform where mobile users make use of cloud services on mobile devices. The use of MCC minimizes the performance, compatibility, and lack of resources issues in mobile computing environment. Despite the astonishing advancement achieved by MCC, the users of MCC are still below expectations because of the associated risks in terms of security and privacy. These risks are playing important role by preventing the organizations to adopt MCC environment. Significant amount of research is in progress in order to reduce the security concerns but still a lot work has to be done to produce a security prone MCC environment. This paper presents a comprehensive literature review of MCC and its security issues and challenges.

Rajkumar Buyya et al.[12] analyze Cloud computing and its aim is to power the next generation data centers and enables application service providers to lease data center capabilities for deploying applications depending on user QoS (Quality of Service) requirements.Cloud applications have different composition, configuration, and deployment requirements. Quantifying the performance of resource allocation policies and application scheduling algorithms at finer details in Cloud computing environments for different application and service models under varying load, energy performance (power consumption, heat dissipation), and system size is a challenging problem to tackle. To simplify this process, in this paper we propose CloudSim: an extensible simulation toolkit that enables modelling and simulation of Cloud computing environments. The CloudSim toolkit supports modelling and creation of one or more virtual machines (VMs) on a simulated node of a Data Center, jobs, and their mapping to suitable VMs. It also allows simulation of multiple Data Centers to enable a study on federation and associated policies for migration of VMs for reliability and automatic scaling of applications.

Cong Wang et al.[13] Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s).Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

Joshi Ashay Mukundrao[14] worked on Cloud computing which is emerging field because of its performance, high availability, least cost and many others. In cloud computing, the data will be stored in storage provided by service providers. But still many business companies are not willing to adopt cloud computing technology due to lack of proper security control policy and weakness in safeguard which lead to many vulnerability in cloud computing. This paper has been written to focus on the problem of data security. Service providers must have a viable way to protect their clients' data, especially to prevent the data from disclosure by unauthorized insiders. To ensure the security of users' data in the cloud, we propose an effective and flexible scheme with two salient features,opposing to its predecessors. Avoiding unauthorized access to user's data by signaling user by sending message to his/her mobile number at the start of transaction. Displaying fake information in case of unsuccessful login for avoiding further login trials by intrusion (Honeypot).

Mohit Marwaha and Rajeev Bedi[15] discuss Cloud computing as it is the next big thing after internet in the field of information technology; some say it's a metaphor for internet. It is an Internet-based computing technology, in which software,shared recourses and information, are provided to consumers and devices on-demand, and as per users requirement on a pay per use model. Even though the cloud continues to grow in popularity, Usability and respectability, Problems with data protection and data privacy and other Security issues play a major setback in the field of Cloud Computing. Privacy and security are the key issue for cloud storage. Encryption is a well known technology for protecting sensitive data. Use of the combination of Public and Private key encryption to hide the sensitive data of users, and cipher text retrieval. The paper analyzes the feasibility of the applying encryption algorithm for data security and privacy in cloud Storage.

Xiaorui Chan and Guangzhong Liu[18] had devised one 160 bits improved hash algorithm based on MD5 and SHA1. And in additional, we also introduce four assistant functions named F(X,Y,Z), G(X,Y,Z), H(X,Y,Z), and I(X,Y,Z) to do 4 rounds of 16 steps iterative operation with 32-bit data as input and 32-bit as output, saving in A, B, C, D respectively. Then we use one new extending function K(X,Y,Z) to expand 32-bit A, B, C, D to 40-bit. At last, by combining the result from low-bit AA, we realize the 160-bit hash algorithm. By analysis, we have found that: without increasing the time complexity, the improved algorithm has increased the security better compared with MD5 and SHA1 algorithms.

Dr. Smith Jones[19] worked on Cloud Computing that has become one of the most talked about technologies in recent times and has got lots of attention from media as well as analysts because of the opportunities it is offering. The market research and analysis firm IDC suggests that the market for Cloud Computing services was $16billion in 2008 and will rise to $42billion/year by 2012 . It has been estimated that the cost advantages of Cloud Computing to be three to five times for business applications and more than five times for consumer applications . According to a Gartner press release from June 2008, Cloud Computing will be "no less influential than ebusiness". Cloud computing evokes different perceptions in different people. To some, it refers to accessing software and storing data in the "cloud" representation of the internet or a network and using associated services. To others, it is seen as nothing new, but just a modernization of timesharing model that was widely employed in 1960s before the advent of relatively lower-cost computing platforms. This development eventually evolved to the client/server model and to the personal computer, which placed large accounts of computing power at people's desktops and spelled the demise of time-sharing systems. This paper proposes and implement a new algorithmic approach for cloud security using key based cryptography. This work can be enhanced using hybrid approach by integrating multiple cryptography algorithms.

3. GAP IN STUDY

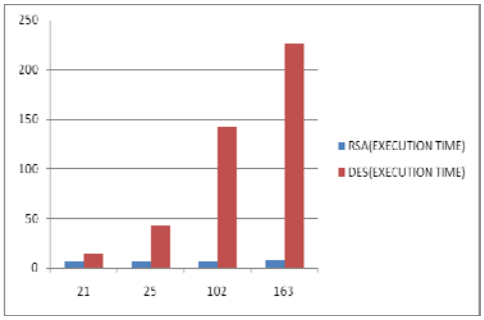
The following observations have been drawn from the literature survey and are listed below:

a) Dual RSA can't be used because the computational complexity of the key generation algorithms was also increased.
b) Many research papers submitted on cryptographic algorithm. Each paper has different perspective.
c) Cryptography can be integrated with cloud computing to increase the security
d) Data can be send on cloud after encryption to increase the security.

4. RESULTS and DISCUSSION

Cryptography is a good way to increase the data security.RSA is better than DES because time taken for encrypting and decrypting data using RSA is much smaller than DES. The time taken by RSA is comparatively constant in front of DES as it can be clearly shown from the following table and graph:

No. of characters	RSA(Execution time in sec.)	DES(Execution time in sec.)
21	6.022	14.134
25	6.833	42.169
102	6.989	142.6
163	7.442	226.481



5. CONCLUSION AND FUTURE SCOPE

After studying various encryption algorithms it is found that RSA is comparatively a good technique as it takes much lesser time and more secure because of its asymmetric nature. Also cloud computing can be used to safely transmission of data and for more safe transmission it is advised to encrypt data first and then transmit the encrypted data through cloud so that if any intermediate user read data, he can only see the encrypted data which is not understandable by him and integrity and confidentiality both remains and data protection increases.

ACKNOWLEDGMENT

The authors are thankful to the H.C.T.M College for providing the platform to work on a positive concept and for their valuable suggestions towards the improvement of paper.

REFERENCES

[1] M. Preetha, M. Nithya," A STUDY AND PERFORMANCE ANALYSIS OF RSA ALGORITHM", IJCSMC, Vol. 2, Issue. 6, June 2013, pg.126 – 139.

[2] AMIT GOYAL and SARA DADIZADEH," A Survey on Cloud Computing"

[3] H. M. Sun, M. E. Wu, W. C. Ting, and M. J. Hinek, "Dual RSA and Its Security Analysis", IEEE Transactions on Information Theory, Vol. 53, No. 8, pp. 2922-2933, 2007.

[4] P.Saveetha & S.Arumugam," Study On Improvement In RSA Algorithm And Its Implementation"

[5] B.Persis urbana ivy,Mukesh kumar,Purshotam mandiwa" A modified RSA Cryptosystem based on n prime numbers",IJECS.

[6] CRS BHARDWAJ Modibada, Jabalpur (Mp), India," Modification Of Des Algorithm", IJIRD, Vol 1 Issue 9, November, 2012, , pg.495 – 505.

[7] Shah Kruti R.& Bhavika Gambhava,"New Approach of Data Encryption Standard Algorithm", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[8] Mary Cindy Ah Kioon, ZhaoShun Wang and Shubra Deb Das," Security Analysis of MD5 algorithm in Password Storage", Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation (ISCCCA-13).

[9] Priyanka Walia & Vivek Thapar," Implementation of New Modified MD5-512 bit Algorithm for Cryptography", international Journal of Innovative Research in Advanced

Engineering (IJIRAE) ISSN: 2349-2163 Volume 1 Issue 6 (July 2014).

[10] C. H. Kim, "Improved Differential Fault Analysis on AES Key Schedule", IEEE Transactions on Information Forensics and Security, Vol. 7, No. 1, pp. 41-50, 2012.

[11] Abid Shahzad and Mureed Hussain,"Security Issues and Challenges of Mobile Cloud Computing",International Journal of Grid and Distributed Computing Vol.6, No.6 (2013), pp.37-50 http://dx.doi.org/10.14257/ijgdc.2013.6.6.04

[12] Rajkumar Buyya, Rajiv Ranjan and Rodrigo N. Calheiros," Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities"

[13] Cong Wang, Qian Wang, and Kui Ren,Wenjing Lou," Ensuring Data Storage Security in Cloud Computing".

[14] Joshi Ashay Mukundrao," Enhancing Security in Cloud Computing" Information and Knowledge Management www.iiste.org ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol 1, No.1, 2011

[15] Mohit Marwaha and Rajeev Bedi," Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013 ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814 www.IJCSI.org

[16] http://en.wikipedia.org/wiki/Cloud_computing.

[17] Atul Khate,Cryptography and network security,second edition.

[18] Xiaorui Chan & Guangzhong Liu," Discussion of One Improved Hash Algorithm Based on MD5 and SHA11", Proceedings of the World Congress on Engineering and Computer Science 2007 WCECS 2007, October 24-26, 2007, San Francisco, USA.

[19] Dr.Smith Jones." AN EMPIRICAL CRYPTOGRAPHY ALGORITHM FOR CLOUD SECURITY BASED ON HASH ENCRYPTION", International Journal of Computing and Corporate Research ISSN (Online) : 2249-054X Volume 4 Issue 4 July 2014 International Manuscript ID : 2249054XV4I4072014-43